

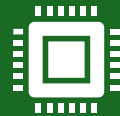


Le VPN Expliqué Simplement et Votre Allié Sécurité en 2025

Qu'est-ce qu'un VPN ?



VPN = Réseau Privé Virtuel



Imaginez un tunnel secret sur Internet : le VPN chiffre vos données et masque votre adresse IP.



Objectif : Protéger votre vie privée et votre sécurité en ligne.



Important : Le VPN est une couche de protection, pas un remplacement pour un antivirus ou un antimalware ou gestionnaire de mots de passe ou authentification à deux facteurs!

À quoi sert un VPN en 2025 ? Partie-1

Qualités (Ce qu'il fait très bien)	Défauts (Ce qu'il fait moins bien)
Confidentialité : Masque votre adresse IP, personne ne sait ce que vous faites en ligne.	Vitesse : Peut ralentir votre connexion (mais les VPN modernes sont de plus en plus rapides).
Sécurité : Chiffre vos données, protège des pirates et des regards indiscrets (surtout sur Wi-Fi public).	Fiabilité : Tous les VPN ne sont pas égaux, certains peuvent même revendre vos données !
Accès : Débloque des contenus géo-restreints (films, séries, sites web) et vous permet de contourner la censure.	Coût : Les bons VPN sont payants (mais il existe des options gratuites avec des limitations).
Anonymat : Rend plus difficile le suivi de vos activités en ligne (mais l'anonymat parfait n'existe pas).	Légalité : L'utilisation d'un VPN est légale dans la plupart des pays, mais certains l'interdisent ou la réglementent (vérifiez les lois locales).
Protection sur Wi-Fi public : Indispensable pour sécuriser vos données dans les cafés, aéroports, etc.	Configuration : Peut être un peu technique pour les débutants (mais les interfaces sont de plus en plus conviviales).
Contournement des restrictions : Accédez à des services bloqués dans votre pays (par exemple, certains réseaux sociaux).	Faux sentiment de sécurité : Un VPN ne vous rend pas invincible, il faut toujours être vigilant (mots de passe, sites web, etc.).
Amélioration de la vitesse : Dans certains cas, un VPN peut même améliorer votre vitesse en contournant les limitations de votre fournisseur d'accès Internet (FAI).	Collecte de données : Certains VPN peu scrupuleux peuvent collecter et revendre vos données (choisissez un VPN de confiance avec une politique de non-journalisation claire).
Protection contre la surveillance : Empêche votre FAI et les autorités de suivre votre activité en ligne.	Blocage par les services : Certains services (Netflix, etc.) détectent et bloquent les adresses IP des VPN.
Meilleure expérience de jeu en ligne : Réduit le ping et le lag dans certains jeux.	Impact sur la batterie : L'utilisation d'un VPN peut consommer plus de batterie sur les appareils mobiles.

À quoi sert un VPN en 2025 ? Partie-2

Qualités (Ce qu'il fait très bien)	Défauts (Ce qu'il fait moins bien)
Facilité d'utilisation : Les applications VPN modernes sont très simples à utiliser, même pour les débutants.	Vulnérabilités : Comme tout logiciel, les VPN peuvent avoir des failles de sécurité (choisissez un VPN qui met régulièrement à jour son application).
Support client : Les meilleurs VPN offrent un support client 24h/24 et 7j/7 en cas de problème.	Implications légales : Dans certains pays, l'utilisation d'un VPN peut être considérée comme illégale ou enfreindre les conditions d'utilisation de certains services.
Compatibilité : Les VPN sont compatibles avec la plupart des appareils (ordinateurs, smartphones, tablettes, routeurs).	Ressources limitées : Les versions gratuites des VPN ont souvent des limitations de vitesse, de données et de serveurs disponibles.
Options de personnalisation : Certains VPN offrent des fonctionnalités avancées (kill switch, double VPN, etc.) pour une protection renforcée.	Manque de transparence : Certains VPN ne sont pas transparents sur leur fonctionnement et leur politique de confidentialité.
Essai gratuit : La plupart des VPN payants proposent une période d'essai gratuit pour tester le service avant de s'engager.	Difficulté de choisir : Il existe des centaines de VPN différents, il peut être difficile de choisir le bon.
Fonctionnalités supplémentaires : Certains VPN offrent des fonctionnalités supplémentaires (bloqueur de publicités, protection contre les malwares, etc.).	Faux VPN : Méfiez-vous des faux VPN qui prétendent offrir un service gratuit mais qui sont en réalité des logiciels malveillants.

À quoi sert un VPN en 2025 ? Partie-3

Qualités (Ce qu'il fait très bien)	Défauts (Ce qu'il fait moins bien)
Multi-plateformes : Un seul abonnement VPN peut être utilisé sur plusieurs appareils.	Contraintes techniques : Certains VPN peuvent être incompatibles avec certains logiciels ou configurations réseau.
Serveurs optimisés : Les VPN modernes proposent des serveurs optimisés pour le streaming, le téléchargement, les jeux en ligne, etc.	Impact sur la navigation locale : Dans certains cas, l'utilisation d'un VPN peut rendre plus difficile l'accès à certains services locaux (sites web de journaux, etc.).
Interface conviviale : Les applications VPN sont généralement très faciles à utiliser, même pour les personnes peu familiarisées avec la technologie.	Besoin d'une connexion internet : Un VPN nécessite une connexion internet pour fonctionner.
Sécurité renforcée : Les meilleurs VPN utilisent des protocoles de chiffrement avancés pour protéger vos données.	Aucune garantie d'anonymat absolu : Même avec un VPN, il est possible de laisser des traces (cookies, empreintes digitales, etc.).
Protection contre le suivi : Empêche les sites web et les annonceurs de vous suivre à la trace.	

Confiance et VPN payants : le revers de la médaille

- **100% confiance ?** Malheureusement, non. Même les VPN payants ne sont pas infaillibles.
- **Cyberattaques ?** Oui, il y a déjà eu des cas de cyberattaques ciblant des fournisseurs de VPN, même payants.
- **Exemples :**
 - En 2020, une faille de sécurité a été découverte dans NordVPN, permettant à un pirate d'accéder à des serveurs.
 - En 2019, des données d'utilisateurs de plusieurs VPN ont été divulguées en raison d'une mauvaise configuration des serveurs.

Pourquoi ces risques ?



Complexité : Les infrastructures VPN sont complexes et peuvent contenir des vulnérabilités.



Attractivité : Les fournisseurs de VPN stockent des données potentiellement intéressantes pour les pirates.



Erreur humaine : Une simple erreur de configuration peut ouvrir la porte aux cyberattaques.

Que faire ?

Choisir un VPN de confiance :

Vérifier la réputation du fournisseur.

Lire les avis d'experts et d'utilisateurs.

S'assurer que le VPN a une politique de non-journalisation claire et transparente.

Préférer les VPN ayant une longue expérience et une bonne réputation en matière de sécurité.

Mises à jour régulières :
S'assurer que le VPN est régulièrement mis à jour pour corriger les failles de sécurité.

Bonnes pratiques :

Utiliser un mot de passe fort et unique pour votre compte VPN.

Activer l'authentification à deux facteurs si elle est proposée.

Ne pas divulguer d'informations personnelles sensibles lorsque vous êtes connecté au VPN.

Rester informé : Se tenir au courant des actualités et des vulnérabilités concernant les VPN.

Conclusion de la première partie

Le VPN est un outil utile pour renforcer votre sécurité et votre vie privée en ligne.

Aucun VPN n'offre une sécurité à 100%, mais un VPN payant de confiance réduit considérablement les risques.

La vigilance reste de mise : même avec un VPN, il est important de rester prudent et de suivre les bonnes pratiques de sécurité.



Conseils supplémentaires pour les aînés

- **Méfiance** : Ne pas cliquer sur des liens suspects ou ouvrir des pièces jointes de personnes inconnues.
- **Mots de passe** : Utiliser des mots de passe forts et différents pour chaque compte.
- **Mises à jour** : Maintenir les logiciels et les systèmes d'exploitation à jour.
- **Sauvegardes** : Effectuer régulièrement des sauvegardes de données importantes.
- **Éducation** : Se tenir informé des dernières menaces et arnaques en ligne.

Pour les personnes ayant un budget limité, voici un tableau comparatif des options de protection, classées par ordre de priorité

Priorité	Type de protection	Justification
1	Antivirus payant	Protection complète contre les malwares, phishing, et autres menaces courantes
2	Antimalware gratuit	Couche de protection supplémentaire, à combiner avec l'antivirus
3	VPN payant	Protection de la vie privée en ligne, mais moins crucial que l'antivirus pour la sécurité de base

Suite: Explication du classement

1. : C'est la base essentielle de la protection en ligne. Les versions payantes offrent une protection en temps réel, des mises à jour régulières et souvent des fonctionnalités supplémentaires comme la protection contre les ransomwares
2. : En complément de l'antivirus payant, un antimalware gratuit comme Malwarebytes peut offrir une couche de protection supplémentaire sans coût additionnel
3. : Bien que utile pour la confidentialité, un VPN est moins crucial pour la sécurité de base que l'antivirus. Il peut être considéré comme un ajout ultérieur si le budget le permet

Pour une protection optimale avec un budget limité, la combinaison recommandée serait :

- Un antivirus payant (ex : Bitdefender, Norton, ou Avast)
- Un antimalware gratuit (ex : Malwarebytes Gratuit)
- Utilisation des VPN gratuits intégrés aux antivirus payants, même s'ils sont limités
- Cette approche offre une protection solide tout en restant abordable pour les aînés disposant d'un budget restreint.

Quel VPN choisir? Avis et comparatifs des meilleurs VPN sur le marché

Publié par: FrançoisCharron.com et daté de février 2025 et Lien pour écouter la vidéo:

<https://francoischarron.com/securite/logiciels-securite-prevention/quel-vpn-choisir-nos-avis-et-comparatifs-des-meilleurs-vpn/KXCKutQ4Nr/>

Ce qu'il dit : heureusement, de plus en plus de gens ont la santé et la sécurité de leur navigation web à cœur et veulent protéger leur connexion internet et leurs données

- Justement, c'est le travail d'un VPN: **chiffrer notre accès à internet** et **crypter les informations qui transitent** entre notre ordinateur, téléphone ou tablette et le site que l'on consulte.
- C'est particulièrement pratique pour **protéger nos informations lorsqu'on est sur un réseau Wi-Fi public** comme dans un café, restaurant ou à l'aéroport par exemple.
- En plus, en se connectant à divers serveurs d'à travers le monde, on peut **contourner les restrictions géographiques** et ainsi continuer d'écouter Netflix au Mexique, Tou.tv en France ou à l'inverse écouter le contenu en ligne de TF1 au Québec

Ses recommandations des meilleures applications VPN à choisir au Canada en 2025 sont... roulement de tambour...



Nom	Site Web	Résumé
NordVPN	https://nordvpn.com/fr/	le VPN polyvalent et performant
Surfshark	https://surfshark.com/fr	un VPN avec le meilleur rapport qualité-prix
CyberGhost	https://www.cyberghostvpn.com/	un VPN optimisé pour le streaming vidéo comme Netflix
ExpressVPN	https://www.expressvpn.com/	un VPN rapide et performant

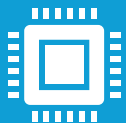
Est-ce que c'est légal d'utiliser un VPN au Canada?



Au Canada, l'utilisation d'un VPN (Virtual Private Network) est légale. Les VPN sont souvent utilisés pour la protection de la confidentialité en ligne, le cryptage des données pour sécuriser les informations sensibles ou l'accès à des contenus avec des restrictions géographiques.



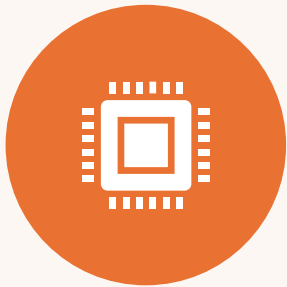
On s'en sert aussi pour accéder à notre compte bancaire ou à des services de streaming pour lesquels on a déjà un abonnement, mais qui sont géographiquement limités (quand on est à l'extérieur du pays en voyage par exemple).



Naturellement, on n'encourage pas l'utilisation d'un VPN pour commettre des actes illégaux, comme le piratage, la fraude, le téléchargement illégal de contenu protégé par les droits d'auteur.

Ces activités sont interdites par la loi et pourraient entraîner des conséquences juridiques.

Est-ce que je devrais choisir un VPN gratuit ou payant pour mon PC, Mac, iOS, iPhone ou Android?



Il existe de nombreux services et fournisseurs de VPN sur le marché, et certains sont payants alors que d'autres sont gratuits.



Cependant, à l'image des antivirus et suites de protection, on est bien mieux servi lorsqu'on opte pour une solution payante.



C'est aussi le cas pour les VPN. Certains VPN gratuits ne cryptent pas tout à fait toutes nos données et nos informations. En fait, certains vont même enregistrer certaines de nos informations comme notre adresse IP, notre modèle d'appareils, etc.





Il faut également faire attention, alors que certains sites de « VPN gratuit » ne sont en réalité que du vent et n'offrent absolument aucune protection.




“Mon” NORDVPN


NordVPN

AUTO-CONNECTÉ
Canada #1214
IP: 185.199.101.34 ISP: PacketHub S.A.





Mettre en pause  


Connexions récentes


-  Connexion Instantanée
-  United States
Serveur le plus rapide
-  Adresse IP dédiée
Canada

Rechercher des connexions 


Pays | Serveurs spécialisés | Appareils

-  Albania
Tirana
-  Algeria
Algiers - Virtuel
-  Andorra
Andorra la Vella - Virtuel
-  Angola
Luanda - Virtuel




Temps de connexion hebdomadaire 




Date	Avec VPN (%)	Sans VPN (%)
06/02	100	0
07/02	50	0
08/02	100	0
09/02	10	0
10/02	100	0
11/02	100	0
12/02	100	0





Protection Anti-menaces Pro™  Gérer

Menaces détectées (30 derniers jours)

-  Fichiers malveillants
0 →
-  Sites web malveillants
0 →
-  Publicités et traqueurs
19615 →

Partage de fichiers Voir tous les appareils 

Appareils récents Faites un glisser-déposer ou parcourez les fichiers

-  michel.doutier27-alps.nord
Hors ligne Envoyer 
-  michel.doutier27-himalayas.nord
Hors ligne Indisponible 

Ma facturation – partie 1

Inclus dans votre abonnement

Actif



NordVPN

Renouvellement automatique

Activé [Annuler](#)

Renouvellement le

novembre 29, 2025 ⓘ

Prochaine facturation

novembre 15, 2025 ⓘ

Tarif de renouvellement

206,28 \$CA/an ⓘ

Mode de paiement



Ma facturation – partie 2

Inclus dans votre abonnement

Actif



Adresse IP dédiée

Renouvellement automatique

Activé [Annuler](#)

Renouvellement le

mai 28, 2025 ⓘ

Prochaine facturation

mai 14, 2025 ⓘ

Tarif de renouvellement

44,77 \$CA / 6 months

Mode de paiement



Date	Abonnement	Mode de paiement	Montant
15/11/2024	1 an NordVPN	Credit card	201,48 \$CA
14/11/2024	6 mois Adresse IP dédiée	PayPal	43,77 \$CA
28/05/2024	6 mois Adresse IP dédiée	PayPal	43,77 \$CA
15/11/2023	1 an NordVPN	Credit card	99,00 \$US
02/04/2023	1 an NordPass	Credit card	18,37 \$CA
19/10/2020	3 ans NordVPN	Credit card	89,00 \$US
29/11/2017	3 ans NordVPN	PayPal	99,00 \$US

Ma facturation et historique – partie 3

NordVPN et ses offres d'abonnements

Choisissez la durée de votre nouvel abonnement

Abonnement 2 ans Abonnement 1 an Abonnement mensuel

Ultra

Économisez 73%

9,69 \$CA/mois

~~873,36 \$CA~~ 232,56 \$CA
pour les 24 premiers mois
La TVA peut s'appliquer

Souscrivez Ultra

Premium

Économisez 70%

7,49 \$CA/mois

~~606,96 \$CA~~ 179,76 \$CA
pour les 24 premiers mois
La TVA peut s'appliquer

Souscrivez Premium

Recommandé pour vous

Avancé

Économisez 70%

6,09 \$CA/mois

~~496,56 \$CA~~ 146,16 \$CA
pour les 24 premiers mois
La TVA peut s'appliquer

Souscrivez Avancé

Basique

Économisez 70%

4,69 \$CA/mois

~~386,16 \$CA~~ 112,56 \$CA
pour les 24 premiers mois
La TVA peut s'appliquer

Souscrivez Basique

Recherches et mise en page par:
ChatGPT, Perplexity, Gemini et Claude
supervisé par:
Michel Cloutier
CIVBDL
Rencontre Zoom
mercredi 12 février 2025
“C’est ensemble qu’on avance”

Annexe – 1

Test VPN exécutés par AV Comparatives, Autriche



<https://www.av-comparatives.org/>

À propos de nous

AV-Comparatives est une organisation indépendante qui propose des tests systématiques pour vérifier si les logiciels de sécurité, tels que les produits antivirus pour PC/Mac et les solutions de sécurité mobile, tiennent leurs promesses. En utilisant l'une des plus grandes collections de menaces au monde, elle crée un environnement réel pour des tests vraiment précis. AV-Comparatives propose des résultats librement accessibles aux particuliers, aux organismes de presse et aux institutions scientifiques. La certification par AV-Comparatives fournit un label officiel d'approbation des performances logicielles qui est reconnu mondialement.

L'histoire d'AV-Comparatives a commencé comme pour beaucoup d'utilisateurs d'ordinateurs, à savoir avec une infection virale. En 1993, [Andreas Clementi](#) a été touché par un virus informatique : le « virus du 17 novembre – NOV_17.855 ». Cela a éveillé son intérêt. Andreas n'était pas satisfait des tests parfois très contradictoires des programmes antivirus dans les magazines informatiques, et a ainsi commencé une enquête intensive sur les logiciels malveillants et les logiciels antivirus, qui se poursuit encore aujourd'hui. En 1999, il a fondé AV-Comparatives avec [Peter Stelzhammer](#) dans le cadre d'un projet étudiant à l'Université d'Innsbruck. Il l'a fait uniquement par intérêt technique, pour voir à quel point les produits des différents fabricants étaient réellement bons. La réponse a été énorme, car les fabricants de logiciels antivirus ont remarqué le duo à Innsbruck et ont voulu participer aux tests.

Annexe - 1, suite et rapport VPN en 2020 Titre: **35** **services VPN mis à l'épreuve**

- Introduction
- L'objectif de ce test est de comparer les services VPN destinés aux consommateurs dans un environnement réel en évaluant leurs fonctionnalités de sécurité et de confidentialité, ainsi que la vitesse de téléchargement, la vitesse de téléversement et la latence.
- Ce rapport commence par une discussion approfondie sur les VPN en général, les différentes applications disponibles de nos jours, ainsi que les avantages et les risques possibles liés à l'utilisation d'un VPN.
- Nous expliquerons plus en détail pourquoi les fournisseurs de VPN doivent avoir une *politique stricte de non-journalisation* . Le rapport est destiné à aider les lecteurs à trouver un programme VPN qui correspond à leurs besoins individuels.

